

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF
TWO MOBILE TELEPHONES
CURRENTLY LOCATED AT THE
SALT LAKE CITY FIELD OFFICE OF
THE FEDERAL BUREAU OF
INVESTIGATION

Case No.2:23mj176 JCB

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Matt Larson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Special Agent (SA) of the Federal Bureau of Investigation (FBI) for twenty-two years. Prior to FBI service, I was a Police Officer for six years. During the past twenty-eight years I have investigated criminal violations related to homicide, rape, child sexual assault, aggravated robbery, aggravated assault, bank robbery, public corruption of government officials, organized crime, drug trafficking, money laundering, firearms trafficking, civil rights, and online sexual exploitation of

children which have resulted in hundreds of felony prosecutions and convictions in several federal and state jurisdictions. In the course of these investigations I have utilized or participated in a variety of traditional and sophisticated investigative techniques to include undercover operations; online undercover operations; wire taps; pen registers; physical surveillance; consensual recordings; interviews and interrogations; recruitment and deployment of informants; search warrants for a variety of evidence to include searches of smart devices, mobile telephones, computers and internet applications; and analysis of evidence contained in telephone records, smart devices, and internet applications. I am currently assigned to the Salt Lake City FBI Child Exploitation Task Force (CETF) where my duties include conducting covert online investigations to identify preferential sex offenders who target juvenile victims. I have also gained experience with internet related investigations as criminal suspects have increased their use of internet tools to facilitate criminal conduct and received related training. In addition, I have owned and used smart devices, mobile telephones, and computers on a daily basis for years and have gained familiarity with them through daily use.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. My knowledge of the information provided below is based on my review of relevant documents and reports and conversations with witnesses and government employees.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched consists of two mobile telephones: a blue Cricket device (IMEI 351244760647304) and a Samsung device in a red and black case (IMEI 356424980594602), hereinafter the “Devices.” The Devices are currently secured at the Salt Lake City Field Office of the FBI, 5425 West Amelia Earhart Drive, Salt Lake City, Utah.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Summary: On May 19, 2022, EARNEST ALLEN, Jr., a federal inmate, escaped from custody and remained an escapee until his arrest on June 2, 2022, when he was booked into the Salt Lake County Jail (ADC). On June 8, 2022, ALLEN was charged in this district by indictment with Escape in violation of 18 USC 751(a). He remains a federal inmate held at the Salt Lake County Jail. At the time of his escape, he was serving a 132 month sentence (ordered on February 13, 2016) and was housed at the Geo Re-entry Facility (Geo) in Salt Lake City, which functions as a federal halfway house. The day before ALLEN escaped, Geo staff seized the devices from ALLEN after he violated cell phone restrictions imposed on him as a convicted sex offender and federal inmate. One of the devices was unlocked. On that device, Geo staff located what appeared to be

child sexual assault material (CSAM). The other device was locked and staff were unable to search the phone as they normally would according to their standard operating procedures. On May 19, Geo staff notified the FBI of possible CSAM on the devices and FBI SA Matt Larson and SA Jeff Ross responded to the facility to investigate. Staff gave the devices to SA Jeff Ross and showed SA Ross where in the phone they had located the suspected CSAM. The devices remain in the custody of the FBI. Although some investigators or contractors of the United States Department of Justice Bureau of Prisons (US BOP) might have the authority to search the devices, and Geo staff have cursorily searched one of the devices and shared that information with agents, your affiant, in an abundance of caution, seeks a search warrant to permit a complete forensic search of both devices for evidence related to the possession, production, or transmission of CSAM.

ADDITIONAL DETAILS

7. According to online court records for the United States District Court (USDC), Southern District of California, on February 13, 2016, ALLEN was sentenced to 132 months imprisonment in the custody of the United States Bureau of Prisons (US BOP) as part of a rule 11 plea agreement wherein he agreed to plead guilty to one count of Enticement of a Minor in violation of 18 USC 2422(b). According to court records, ALLEN was originally charged with the following violations: Sex Trafficking of Children [18 USC 1591(a) and (b) and 18 USC 2253]; Sexual Exploitation of a Child [18

USC 2251(a)]; and, Possession of Images of Minors Engaged in Sexually Explicit Conduct [18 USC 2252(a)(4)(B)].

8. According to Geo records I have reviewed, on January 26, 2022, ALLEN was granted residence at a Geo Reentry Services (Geo) facility at 1585 West 2100 South, Salt Lake City, Utah, as a federal inmate in the custody of the US BOP. Geo provides corrections services to state and federal government corrections agencies. This location has served as a federal “half way house” under the management of various organizations for many years.

9. On May 19, 2022, FBI SA Matt Larson and FBI SA Jeff Ross responded to the Geo facility at the request of staff to investigate a report that ALLEN possessed CSAM on his cell phone and had escaped from custody as a federal inmate. The agents interviewed Geo facility director Leslie Flowers and other staff members and obtained copies of agreements signed by ALLEN as a condition of his acceptance at the facility. Regarding the forms I reviewed, in summary they establish ALLEN was still a US BOP inmate while housed at the Geo facility and was subject to the search of his person and possessions when in or re-entering the facility, that he was prohibited from possessing or using smart phones and that he could only possess a “flip phone” if that particular phone was authorized and inventoried by staff. The agents also obtained a copy of a written “US DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF PRISONS INCIDENT

REPORT” form submitted by Geo Case Manager Rodney Priest regarding the CSAM allegation which is substantially reproduced in the following paragraph.

10. The narrative portion of Priest’s report contains the following information: “On 18 May 2022 at 2:14pm inmate Allen, Earnest, reg# 38542-298, signed into the facility; staff searched his person and property. Staff discovered an unauthorized Smart phone in his backpack. This item was confiscated and brought to Administration; this item was subsequently turned over to his Case Manager. On 18 May at 3:30pm I reviewed the contents of the phone. I discovered no fewer than 10 downloaded videos containing pornography; all of these videos contain nudity and/or individuals performing sex acts on others. On one of the videos titled “daddy_fucks_daughter” I discovered the image of a female person, who clearly appears to be a minor, performing sexual acts on an adult male. Date and Time: 5-19-22 11:14am; Name and Title: R. Priest CM2.”

11. Flowers also provided a copy of a form signed by ALLEN titled “REQUEST FOR AUTHORIZATION OF CELLULAR TELEPHONE.” That form is dated January 31, 2022, in the name of EARNEST ALLEN for a Cricket “flip phone” (“flip phone” is hand written in the field for Make/Model), and lists the telephone number 385-296-2907. Under the heading “Resident Review and Agreement (all boxes must be initialed by resident)” the following conditions are listed next to boxes. The boxes are all checked.

- a. I understand I will be allowed to have a smartphone (if appropriate) for the purpose of communicating with Potential Employers, Educators, Family, Friends, and other members of the community.
- b. I will not lock my smartphone/cellular phone at any time.
- c. I will allow RRC staff to have access to my account. This includes pass codes if applicable.
- d. Smartphone/Cellular telephones must stay on vibrate at all times.
- e. Staff may ask to look at your phone at any time for audit purposes. If you refuse your phone will be confiscated and level dropped to a 2.
- f. Nude or pornographic photographs or text of a sexual nature is prohibited and are grounds for confiscation of the cellular phone. GANG related pictures or symbols will NOT BE tolerated!!
- g. Taking pictures of staff or other residents is forbidden.
- h. Cellular phones may be used until curfew.
- i. Be respectful of others: don't talk loud in cubes, living areas, etc.
- j. No cellular phone usage during chores, in the lobby, or during emergency drills/evacuations.
- k. Phone chargers are not allowed to be plugged in while not in use.

- l. If a cellular phone is confiscated at any time, you will not get it back until disciplinary sanctions have been completed, and/or at administrations discretion.
- m. You may not lend or borrow cell phones to or from other residents. The phone will be confiscated and not returned until disciplinary sanctions have been completed, and/or at administrations discretion.
- n. Resident call-ins while on pass still need to be made from a landline not your cellular phone.
- o. Changing cellular phones without staff permission is prohibited.
- p. Current copy of cell phone bill must be turned in with the Monthly Financial Reports.
- q. Cell phones must be brought to all Case Manager Meetings for audit purposes.
- r. Residents are not allowed to contact other residents on the cell phone in any form, for any reason. (ex texting, picture sending or talking)
- s. I understand misuse or abuse of the smartphone privileges and/or violation of any of the above rules may result in an Incident Report, and a request to revoke your privileges will be submitted to the RRM.

t. I have read and understand the above SLC Smartphone Policy; Failure to comply will result in loss of smartphone privileges.

u. Signed by Earnest Allen on 1-31-22.

12. Flowers stated that as a convicted sex offender and federal inmate, ALLEN was not permitted to possess a smart phone under any conditions while a resident at the facility. The only type of phone permitted to him was a “flip phone” or a phone that is not a smart device with internet search capability. Neither of the Devices seized from ALLEN comply with the above agreement. The device in the red and black case was possessed without any request and as a smart phone is prohibited contraband for ALLEN under any circumstances. The blue phone was a Cricket phone, like the device referred to on the form ALLEN filled out, but it is not a flip phone as described on the cell phone request form with no internet access, it is a smart phone with internet access.

13. On May 18, 2022, ALLEN returned to the facility after an authorized absence and facility monitor Kevin Sonntag checked ALLEN in according to standard operating procedures. Sonntag searched ALLEN and items in his possession according to facility protocols. During the search, Sonntag located a blue Cricket smartphone in a backpack ALLEN brought into the facility. During the search, Sonntag observed that ALLEN had a second cell phone in a red and black case in his possession. Sonntag seized the blue Cricket phone but not the other phone because at the time he thought ALLEN was authorized to have the phone in the red and black case but not the Cricket phone.

Sonntag later realized the phone in the red and black case was a contraband item. Later that evening, May 18, 2022, the cell phone in the red and black case was seized by Geo staff member Angelo Clelan because ALLEN was not authorized to have it.

14. On May 19, 2022, Sonntag and Priest reviewed the blue Cricket phone together. During that review, Sonntag located a video he believed to depict an adult male having sexual intercourse with a juvenile female. Priest located a conversation in Google Hangouts as well where messages on the phone contained internet links. One of the links was to a page which displayed a video titled “Daddy_fucks_daughter” which depicted a female Priest believed to be between 14 and 16 years old engaged in oral sex with an adult man.

15. Flowers advised the agents ALLEN was required to return to the Geo facility at 3:00 PM that day, May 19th, 2022. ALLEN was required by contract to return to the facility on time every time he left. Federal inmates like ALLEN were reported to US BOP as escaped prisoners whenever late by 20 minutes or more. At the time agents concluded contact with Geo staff on May 19th, it was 4:00 PM, ALLEN was late without excuse for 60 minutes and Geo had reported him as an escaped prisoner. ALLEN remained an escapee until June 2, 2022, when he was arrested by the United State Marshall Service and FBI and booked into the Salt Lake County Adult Detention Center/Jail (ADC). On June 8, 2022, ALLEN was formally charged by indictment in this district with Escape.

16. Flowers had ALLEN'S Devices in her office when the agents were interviewing her. Sonntag accessed the blue Cricket phone and showed the agents some of the material he thought was illegal CSAM. The females in the material Sonntag showed us did appear to be teenage girls. Based on the conduct of ALLEN regarding the phones, his history as a sexual predator with a sexual interest in the exploitation of juvenile girls, my conversations with SA Ross and my own training and experience, there is probable cause to believe ALLEN used the blue Cricket phone to access, view, possess or store CSAM. The other phone seized from ALLEN, the one in the black and red case, has not been examined.

17. Both devices were seized from ALLEN at the Geo facility. The Cricket phone was unlocked in accordance with the written cell phone agreement. The other device was locked and could not be reviewed. The unlocked device contains pornographic material that appears to be CSAM. Given that ALLEN is a preferential sex offender with a sexual interest in children and that he has a history of producing CSAM while he sexually assaults juvenile girls my training and experience informs me that the locked device is likely to contain CSAM as well. The CSAM on the unlocked phone suggests ALLEN still has a sexual interest in juvenile females. Under the circumstances both devices were contraband for ALLEN, both may contain CSAM and both devices should be searched for evidence related to the possession, transmission or production of CSAM.

18. The Devices are currently in storage at the Salt Lake City FBI Field Office Evidence Control Room. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates,

appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable

media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless

communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer or digital files or remnants of such files can be recovered months or even years

after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer or electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. In addition, an electronic device user may delete a file such as a video or photograph from one location on an electronic device but the same file may appear in another location on the device.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal memory storage —contain electronic evidence of how a computer or electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts

from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of the use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online nicknames and passwords. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to possess, produce, receive or distribute CSAM, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Matt Larson

MATT LARSON
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 on February 27, 2023:



JARED C. BENNETT
United States Magistrate Judge

ATTACHMENT A

The property to be searched consists of two mobile telephones: a blue Cricket device (IMEI 351244760647304) and a Samsung device in a red and black case (IMEI 356424980594602), hereinafter the “Devices.” The Devices are currently secured at the Salt Lake City Field Office of the FBI, 5425 West Amelia Earhart Drive, Salt Lake City, Utah.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 USC 2252A (Certain activities related to material constituting or containing child pornography) and involve Earnest Allen, Jr., between January 1, 2022 and June 2, 2022, including:

- a. Photograph or video files containing CSAM.
- b. Text messages or communications in messaging applications used to possess, produce, search for, or distribute CSAM.
- c. Evidence tending to identify access to websites, internet addresses or applications used to possess, produce, search for, or distribute CSAM.
- d. Evidence tending to identify when, where and for how long the ALLEN used the devices to violate the listed statute.
- e. identifying information related to other persons ALLEN communicated with to violate the listed statute.
- f. browsing history or search history related to conduct prohibited in the listed statute.
- g. any information related to sources of CSAM (including names, addresses, phone numbers, or any other identifying information);

- h. all bank records, checks, credit card bills, account information, and other financial records related to ALLEN'S payment for CSAM or payment for subscription to websites or applications used to violate the listed statute.
 - i. Evidence related to the purchase of other electronic devices or storage media.
 - 2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
 - 3. Records identifying Internet Protocol addresses used to violate the listed statute including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.